

Prior to entry of this paper, Claims 1-20 were pending. Claims 1-20 were rejected. In this paper, Claims 1-10, 12-13, 18-20 are amended; no claims are canceled; and no claims are added. Claims 1-20 are currently pending. No new matter is added by way of this amendment. For at least the following reasons, Applicants respectfully submit that each of the presently pending claims is in condition for allowance.

Claims 18, 19 have been rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. In response, the Applicants have amended claims 18-19 to recite a network device for managing content in a highly distributed system. Because a network device is directed towards statutory subject matter under 35 U.S.C. §101, the rejection is now moot, and should be withdrawn.

Claims 1-3, 5-8, 10, 11 are rejected under 35 U.S.C. 102(e) as being anticipated by Benaloh et al. (US Patent No. 7,065,216). Claims 4, 9, 12-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Benaloh in view of Cooper et al (US PG PUB No. 20010051996). The Applicants respectfully traverse these rejections.

Applicants submit that the cited prior art references do not teach or suggest each of the limitations of at least amended claim 1. For example, amended claim 1 recites, in part, determining a self-identifier that uniquely identifies an entity decrypting the content, and modifying the decrypted content by embedding at least one of a fingerprint or watermark into the decrypted content, where the fingerprint or watermark is generated in part from the self-identifier. The Applicants respectfully submit that Benaloh does not teach or suggest such limitations.

Instead, Benaloh teaches methods and systems that enable protection of digital content by making pirated copies traceable back to a unique decryption key. See Benaloh Abstract. Benaloh discloses using multiple different keys to decrypt the content such that, when the different keys are utilized to decrypt the content, the decrypted versions of the content will indicate which key, and hence, the content play from which it came. See Benaloh Col. 5, lines 50-55. For example, as shown in figure 4 of Benaloh, is an encrypted content package 400 which includes the encrypted content 304 and a so-called encrypted content key assembly 402. The encrypted content key assembly 402 contains multiple encrypted content keys 318a-N – one for each valid content player....the encrypted content key assembly contains an encrypted content key for each content player. See Benaloh, Col 7, lines 1-11. The player is advantageously configured to find the content key(s) that have been encrypted with its public device key 314 (Fig. 3 of Benaloh). Only authorized content players are able to access the encrypted content key because the unauthorized content player will not have an associated private device key to decrypt the associated encrypted content key(s). See Benaloh, Col. 7, lines 35-47.

Furthermore, Benaloh teaches partitioning the content into multiple partitions, each of the individual partitions of a partition set is then separately and uniquely marked. See Benaloh, Col. 9, lines 1-15. Individual different keys are then associated with each of the uniquely marked partitions. Individual unique key collections are defined in which in any one key collection, there appears one and only one key for one partition or clip in each partition set. In the illustrated example, no two key collections are the same. Each unique key collection is then associated with a corresponding content player and encrypted with the content player's device key. See Benaloh, Col. 9, line 45 through Col. 10, line 19.

Thus, what Benaloh teaches is using unique key collections of uniquely marked content partitions to trace content to a content player. That is, no two content players have exactly the same key collection. As such, it logically follows that each content player, by virtue of using its unique key collection, is presented with a slightly different version of marked content. See Benaloh, Col. 10, line 63 - Col. 11, line 12. Thus, Benaloh teaches that tracing is based on the unique key

In fact, Benaloh actually teaches away from using a fingerprint or watermark that is generated from a unique identifier associated with the entity decrypting the content. See for example, Benaloh at Col 5, lines 22-33, where it states that “[o]ne past software solution which is less than ideal is to specially mark each digital content copy...with its own unique identifier and to associate the marked copy with a particular airline or airplane. Specifically, serially marking each copy of a movie is a tedious and undesirably expensive process.” (Emphasis Added). Thus, Benaloh, instead teaches using a unique combination of marked partitions of content and a unique collection of keys to trace the content.

However, Benaloh also does not teach or suggest wrapping the encrypted modified content together with the self-identifier using an access key. While Benaloh does disclose a device key pair that is associated with a single device player, the device key pair is not used as a self-identifier to generate a fingerprint or watermark as recited by at least Applicants' claim 1. See Benaloh, Col 6, lines 1-65. Moreover, it would not be consistent for the Benaloh's device key pair to then be used to wrap the encrypted modified content together with the device key pair using the device key pair, as would appear to be required to conform Benaloh to at least claim 1. Thus, for at least this reason, Benaloh does not anticipate nor render obvious at least claim 1 of the Applicants. Furthermore, Cooper combined with Benaloh (the combination which would be incompatible and improperly

modify the principle of operation of Benaloh) also does not appear to resolve these issues. Therefore, Applicants respectfully request that at least claim 1 be allowed to issue.

Independent Claims 12, 18, and 20 include similar, albeit different, limitations of Claim 1. For example, Claim 18 recites a first wrapper that includes encrypted content, a first identifier that uniquely identifies a first market participant. Claim 18 further recites generating a second wrapper that wraps the content key, the encrypted marked content, the first unique identifier, and a second unique identifier that uniquely identifies the second market participant. The encrypted marked content being marked by embedding the fingerprint or watermark into the decrypted content, where the fingerprint or watermark is generated to uniquely identify the second market participant. Neither Benaloh nor Cooper, alone or in combination (the combination of which the Applicants deny) teach or suggest at least these limitations of Claim 18.

Independent Claim 12 similarly recites a self-identifier that uniquely identifies the recipient of the content, generating a fingerprint in part from the self-identifier, and watermarking the content employing the fingerprint. Again, neither Benaloh nor Cooper, alone or in combination teach or suggest at least these limitations. Furthermore, Claim 20 also recites an identifier that uniquely identifies the entity decrypting the content, and modifying the decrypted content by embedding at least of a fingerprint or watermark generated from the unique identifier. Benaloh alone or in combination with Cooper does not teach or suggest at least these limitations. Thus, the Applicants respectfully submit that the cited prior art references fail to anticipate or render obvious at least claims 1, 12, 18, and 20. Therefore, the Applicants respectfully request that these claims be allowed to issue.


Moreover, claims 2-11, 13-17, and 19 depend from claims 1, 12, and 18, respectively. Therefore, they are also allowable for at least the same reasons as claims 1, 12, and 18. Therefore, the Applicants request that these dependent claims also be allowed to issue.

CONCLUSION

It is respectfully submitted that each of the presently pending claims (Claims 1-20) are in condition for allowance and notification to that effect is requested. Examiner is invited to contact the Applicants' representative at the below-listed telephone number if it is believed that the prosecution of this application may be assisted thereby. Although only certain arguments regarding patentability are set forth herein, there may be other arguments and reasons why the claimed invention is patentable. Applicants reserve the right to raise these arguments in the future.

Dated: August 20, 2007

Respectfully submitted,

By 

Jamie L. Wiegand

Registration No.: 52,361

DARBY & DARBY P.C.

P.O. Box 770

Church Street Station

New York, New York 10008-0770

(206) 262-8915

(212) 527-7701 (Fax)

Attorneys/Agents For Applicant